(19) EuropäischesPatentamt
EuropeanPatentOffice
Officeeuropéendesbrevets

(11) EP 0661845 A3

(12) EUROPEANPATENTAPPLICATION

(88) DateofpublicationA3:
01.03.2000 Bulletin 2000/09

(43) DateofpublicationA2:
05.07.1995 Bulletin 1995/27

(21) Applicationnumber: **94309658.6**

(22) Dateoffiling: **21.12.1994**

(51) IntCl.[7]: **H04L 9/32**,H04L 9/30

(84) DesignatedContractingStates:
DEFRGB

(30) Priority: **29.12.1993 US 175024**

(71) Applicant: **InternationalBusinessMachines Corporation**
Armonk,N.Y.10504(US)

(72) Inventors:
- **Dwork,Cynthia**
  PaloAlto,California94301(US)
- **Naor,Simeon**
  Tel-Aviv,69122(US)

(74) Representative: **Moss,RobertDouglas**
IBMUnitedKingdomLimited
IntellectualPropertyDepartment
HursleyPark
WinchesterHampshireSO212JN(GB)

(54) Systemandmethodformessageauthenticationinanon-malleablepublic-keycryptosystem

(57) Amethodisprovidedforauthenticationofencryptedmessages(M).Anon-malleablepublic-keyencryptiontechniqueisemployed,sothataneavesdropper(B)cannotemployanencryptedmessage(M),previouslyoverheard,togenerateamessagewhich,when senttoarecipient(R),whichwouldpassasamessage originatingfromavalidsender(S).Inapreferredembodiment,aprotocolisprovidedinwhich,inresponse toamessageauthenticationrequest(req)fromasender,arecipient(R)sendsthesender(S)astring(st),encryptedaccordingtothesender'snon-malleablepublic key(Es).Thesender(S)decryptsthestringusingits private key, and sends the recipient (R) a message (Auth(M,ST))whichisafunction(Auth)ofthestring (St)andthemessage(M)tobeauthenticated.Because ofthenon-malleabilityofthepublickeys,aneavesdropper cannotimpersonatethesender(S)ortherecipient (R)andproduceadisinformationmessagewhichwould neverthelesscontainthecorrectauthorizationstring.

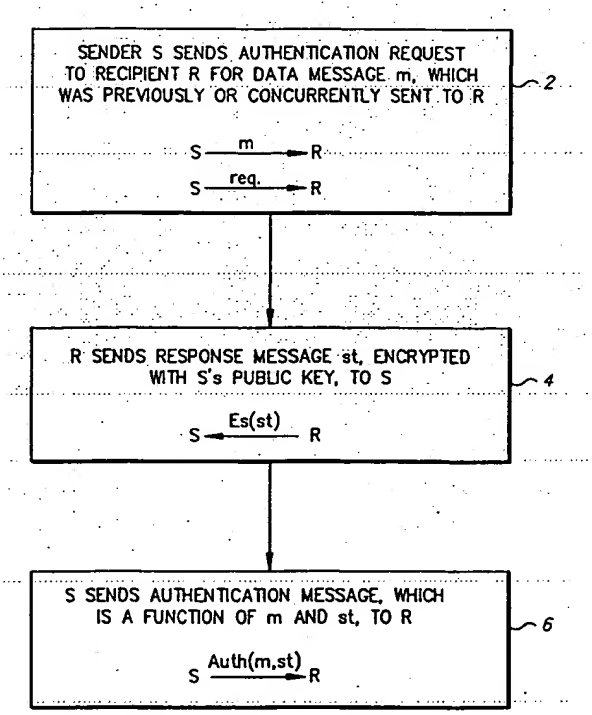

FIG. 2

EP 0 661 845 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 30 9658

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 522 473 A (MITSUBISHI ELECTRIC CORP) 13 January 1993 (1993-01-13) * abstract * * column 1, line 50 - column 2, line 20 * * column 4, line 52 - column 7, line 2 * * claim 1 * * figures 2,4 *	1,2,4,5	H04L9/32 H04L9/30
A	SIMMONS G J: "A PROTOCOL TO PROVIDE VERIFIABLE PROOF OF IDENTITY AND UNFORGEABLE TRANSACTION RECEIPTS" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS,US,IEEE INC. NEW YORK, vol. 7, no. 4, page 435-447 XP000007982 ISSN: 0733-8716 * abstract * * page 436, right-hand column, line 6 - line 20 * * page 437, right-hand column, line 3 - line 33 * * page 439, right-hand column, line 22 - page 442, right-hand column, line 47 *	1-6	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	10 January 2000	Gautier, L

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 94 30 9658

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

10-01-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0522473 A	13-01-1993	JP 2671649 B	29-10-1997
		JP 5012321 A	22-01-1993
		DE 69224238 D	05-03-1998
		DE 69224238 T	20-05-1998
		US 5245657 A	14-09-1993

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82